

Configurando o VPN 3000 Concentrator PPTP com autenticação RADIUS do Cisco Secure ACS para Windows

Contents

[Introduction](#)

[Antes de Começar](#)

[Conventions](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configurando o VPN 3000 Concentrator](#)

[Adição e configuração do Cisco Secure ACS para Windows](#)

[Adicionando MPPE \(Criptografia\)](#)

[Relatório de adição](#)

[Verificar](#)

[Troubleshoot](#)

[Habilitando a depuração](#)

[Depurações - Boa autenticação](#)

[Possíveis erros](#)

[Informações Relacionadas](#)

[Introduction](#)

O Cisco VPN 3000 Concentrator suporta o método de tunelamento PPTP (Point-to-Point Tunnel Protocol) para clientes nativos do Windows. O concentrador suporta criptografia de 40 e 128 bits para uma conexão segura e confiável. Este documento descreve como configurar o PPTP em um VPN 3000 Concentrator com o Cisco Secure ACS for Windows para autenticação RADIUS.

Consulte [Configurando o Cisco Secure PIX Firewall para Usar o PPTP](#) para configurar conexões PPTP com o PIX.

Consulte [Configuração da Autenticação PPTP do Cisco Secure ACS for Windows Router](#) para configurar uma conexão de PC ao roteador; isso fornece autenticação de usuário ao servidor Cisco Secure Access Control System (ACS) 3.2 para Windows antes de permitir que o usuário entre na rede.

[Antes de Começar](#)

[Conventions](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

[Prerequisites](#)

Este documento pressupõe que a autenticação PPTP local está funcionando antes de adicionar a autenticação Cisco Secure ACS para Windows RADIUS. Consulte [Como configurar o VPN 3000 Concentrador PPTP com autenticação local](#) para obter mais informações sobre a autenticação PPTP local. Para obter uma lista completa de requisitos e restrições, consulte [When Is PPTP Encryption Supported on a Cisco VPN 3000 Concentrator? \(Quando a criptografia PPTP é suportada em um Cisco VPN 3000 Concentrador?\)](#)

[Componentes Utilizados](#)

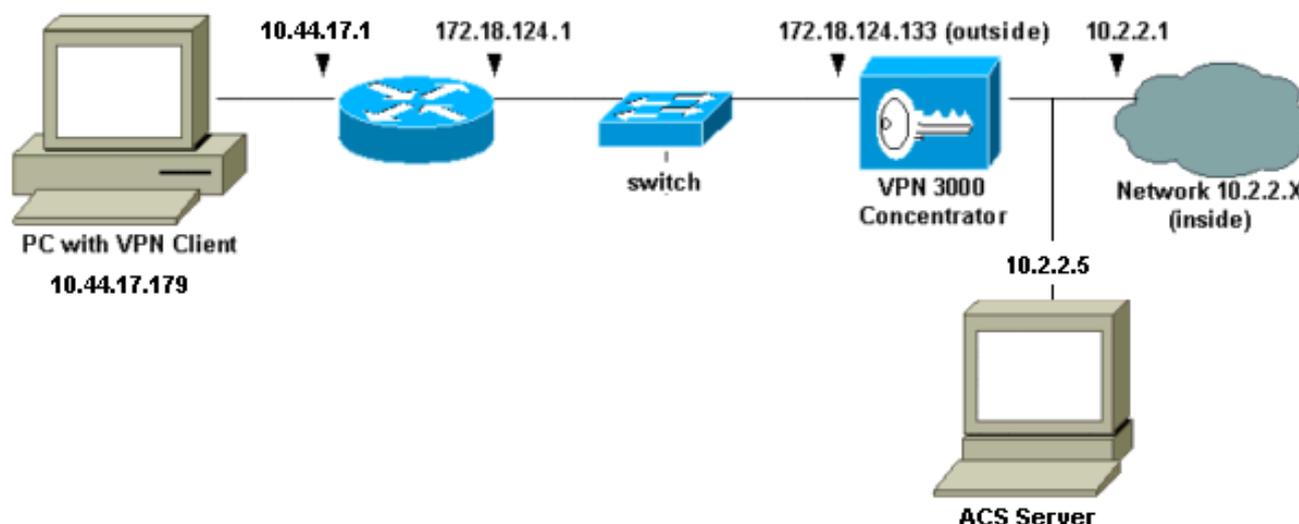
As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Cisco Secure ACS para Windows versões 2.5 e posteriores
- VPN 3000 Concentrador versões 2.5.2.C e posteriores (essa configuração foi verificada com a versão 4.0.x.)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

[Diagrama de Rede](#)

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



[Configurando o VPN 3000 Concentrador](#)

[Adição e configuração do Cisco Secure ACS para Windows](#)

Siga estas etapas para configurar o VPN Concentrador para usar o Cisco Secure ACS for

Windows.

1. No VPN 3000 Concentrator, vá para **Configuration > System > Servers > Authentication Servers** e adicione o servidor e a chave Cisco Secure ACS for Windows ("cisco123" neste exemplo).

The screenshot shows the configuration page for adding a user authentication server. The breadcrumb navigation at the top reads "Configuration | System | Servers | Authentication | Add". Below the navigation, the instruction "Configure and add a user authentication server." is displayed. The "Server Type" dropdown menu is set to "RADIUS". A tooltip points to the dropdown, stating: "Selecting *Internal Server* will let you add users to the internal user database." The "Authentication Server" field contains "10.2.2.5" with the instruction "Enter IP address or hostname." The "Server Port" field contains "0" with the instruction "Enter 0 for default port (1645)." The "Timeout" field contains "4" with the instruction "Enter the timeout for this server (seconds)." The "Retries" field contains "2" with the instruction "Enter the number of retries for this server." The "Server Secret" field contains masked characters with the instruction "Enter the RADIUS server secret." The "Verify" field also contains masked characters with the instruction "Re-enter the secret." At the bottom, there are "Add" and "Cancel" buttons, with a mouse cursor hovering over the "Add" button.

2. No Cisco Secure ACS para Windows, adicione o VPN Concentrator à configuração de rede do servidor ACS e identifique o tipo de

Access Server Setup For VPN3000

Network Access Server IP Address	<input type="text" value="10.2.2.1"/>
Key	<input type="text" value="cisco123"/>
Network Device Group	<input type="text" value="(Not Assigned)"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/>	Single Connect TACACS+ NAS (Record stop in accounting on failure).
<input type="checkbox"/>	Log Update/Watchdog Packets from this Access Server
<input type="checkbox"/>	Log Radius Tunneling Packets from this Access Server

dicionário.

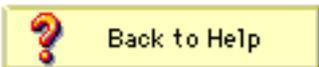
3. No Cisco Secure ACS for Windows, vá para **Interface Configuration > RADIUS (Microsoft)** e verifique os atributos do Microsoft Point-to-Point Encryption (MPPE) para que os atributos apareçam na interface do

Edit

RADIUS (Microsoft)

User Group

- [026/311/007]
MS-MPPE-Encryption-Policy]
- [026/311/008]
MS-MPPE-Encryption-Types
- [026/311/012]
MS-CHAP-MPPE-Keys
- [026/311/016] MS-MPPE-Send-Key
- [026/311/017]
MS-MPPE-Recv-Key

 Back to Help

grupo.

4. No Cisco Secure ACS para Windows, adicione um usuário. No grupo do usuário, adicione os atributos MPPE (Microsoft RADIUS), caso você precise de criptografia

Access Restrictions	Token Cards	Password Aging
IP Address Assignment	IETF Radius	Cisco VPN3000 Radius
MS MPPE Radius		

Microsoft RADIUS Attributes ?

[311\007] MS-MPPE-Encryption-Policy
Encryption Allowed

[311\008] MS-MPPE-Encryption-Types
40-bit

[311\012] MS-CHAP-MPPE-Keys

[311\016] MS-MPPE-Send-Key

[311\017] MS-MPPE-Recv-Key

posteriormente.

- No VPN 3000 Concentrator, vá para **Configuration > System > Servers > Authentication Servers**. Selecione um servidor de autenticação na lista e, em seguida, selecione **Testar**. Teste a autenticação do VPN Concentrator para o servidor Cisco Secure ACS for Windows inserindo um nome de usuário e uma senha. Em uma boa autenticação, o VPN Concentrator deve mostrar uma mensagem "Authentication Successful" (Autenticação bem-sucedida). Falhas no Cisco Secure ACS for Windows estão registradas em **Relatórios e Atividade > Tentativas com Falha**. Em uma instalação padrão, esses relatórios são armazenados em disco em C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts.

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name

Password

OK Cancel

6. Como agora você verificou se a autenticação do PC para o VPN Concentrator funciona e do concentrador para o servidor Cisco Secure ACS for Windows, você pode reconfigurar o VPN Concentrator para enviar usuários PPTP para o Cisco Secure ACS for Windows RADIUS movendo o servidor Cisco Secure ACS for Windows para o topo da lista de servidores. Para fazer isso no VPN Concentrator, vá para **Configuration > System > Servers > Authentication Servers**.

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Authentication Servers	Actions
10.2.2.5 (Radius)  Internal (Internal)	<input type="button" value="Add"/>
	<input type="button" value="Modify"/>
	<input type="button" value="Delete"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>
	<input type="button" value="Test"/>

- Vá para **Configuration > User Management > Base Group** e selecione a guia **PPTP/L2TP**. No grupo base do VPN Concentrator, certifique-se de que as opções para **PAP** e **MSCHAPv1** estejam ativas.

General

IPSec

PPTP/L2TP

PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input checked="" type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

8. Selecione a guia **Geral** e verifique se o PPTP é permitido na seção Protocolos de tunelamento.

Idle Timeout	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect time	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
Filter	<input type="text" value="-None-"/>	Select the filter assigned to this group.
Primary DNS	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
Secondary DNS	<input type="text"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
Secondary WINS	<input type="text"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.

9. Teste a autenticação PPTP com o usuário no servidor Cisco Secure ACS for Windows RADIUS. Se isso não funcionar, consulte a seção [Depuração](#).

[Adicionando MPPE \(Criptografia\)](#)

Se a autenticação do Cisco Secure ACS para Windows RADIUS PPTP funcionar sem criptografia, você poderá adicionar MPPE ao VPN 3000 Concentrator.

1. No VPN Concentrator, vá para **Configuration > User Management > Base Group**.
2. Na seção Criptografia PPTP, verifique as opções para **Obrigatório, 40 bits e 128 bits**. Como nem todos os PCs suportam a criptografia de 40 e 128 bits, verifique as duas opções para permitir a negociação.
3. Na seção Protocolos de autenticação PPTP, marque a opção para **MSCHAPv1**. (Você já configurou os atributos de usuário do Cisco Secure ACS para Windows 2.5 para criptografia em uma etapa anterior.)

PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking all options means that no authentication is required.
PPTP Encryption	<input checked="" type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

Observação: o cliente PPTP deve ser reconhecido para criptografia de dados ideal ou necessária e MSCHAPv1 (se uma opção).

[Relatório de adição](#)

Depois de estabelecer a autenticação, você pode adicionar a contabilidade ao VPN Concentrador. Vá para **Configuration > System > Servers > Accounting Servers** e adicione o servidor Cisco Secure ACS for Windows.

No Cisco Secure ACS para Windows, os registros de contabilidade são exibidos da seguinte forma.

```
Date, Time, User-Name, Group-Name, Calling-Station-Id, Acct-Status-Type, Acct-Session-Id,
  Acct-Session-Time, Service-Type, Framed-Protocol, Acct-Input-Octets, Acct-Output-Octets,
  Acct-Input-Packets, Acct-Output-Packets, Framed-IP-Address, NAS-Port, NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
  PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
  PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

[Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

[Troubleshoot](#)

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

[Habilitando a depuração](#)

Se as conexões não funcionarem, você poderá adicionar classes de eventos PPTP e AUTH ao VPN Concentrator indo-se em **Configuration > System > Events > Classes > Modify**. Você também pode adicionar classes de eventos PPTPDBG, PPTPDECODE, AUTHDBG e AUTHDECODE, mas essas opções podem fornecer muitas informações.

Configuration | System | Events | Classes | Modify

This screen lets you modify an event class configured for special handling.

Class Name	<input type="text" value="PPTP"/>	
Enable	<input checked="" type="checkbox"/>	Check to enable special handling of this class.
Severity to Log	<input type="text" value="1-9"/>	Select the range of severity values to enter in the log.
Severity to Console	<input type="text" value="1-3"/>	Select the range of severity values to display on the console.
Severity to Syslog	<input type="text" value="None"/>	Select the range of severity values to send to a Syslog server.
Severity to Email	<input type="text" value="None"/>	Select the range of severity values to send via email to the recipient list.
Severity to Trap	<input type="text" value="None"/>	Select the range of severity values to send to an SNMP system.

Você pode recuperar o log de eventos indo para **Monitoring > Event Log**.

Monitoring | Event Log

Select Filter Options

Event Class: All Classes (dropdown menu showing AUTH, AUTHDBG, AUTHDECODE)

Severities: ALL (dropdown menu showing 1, 2, 3)

Client IP Address: 0.0.0.0 (text input)

Events/Page: 100 (dropdown menu)

Direction: Oldest to Newest (dropdown menu)

Buttons: <<<, <<, >>, >>>, Get Log, Save Log, Clear Log

1 12/04/2000 14:51:32.600 SEV=4 AUTH/22 RPT=21
User pptpuser disconnected

2 12/04/2000 14:51:32.600 SEV=4 PPTP/35 RPT=14 10.44.17.179
Session closed on tunnel 10.44.17.179 (peer 0, local 45636, serial 0), re
Administrative shutdown (No additional info)

4 12/04/2000 14:51:32.640 SEV=4 PPTP/34 RPT=14 10.44.17.179
Tunnel to peer 10.44.17.179 closed, reason: Stop-Local-Shutdown (No addit
info)

6 12/04/2000 14:51:49.150 SEV=4 PPTP/47 RPT=15 10.44.17.179
Tunnel to peer 10.44.17.179 established

[Depurações - Boa autenticação](#)

As boas depurações no VPN Concentrador serão semelhantes às seguintes.

```

1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected

```

[Possíveis erros](#)

Você pode encontrar possíveis erros, como mostrado abaixo.

[Nome de usuário ou senha incorreta no servidor Cisco Secure ACS for Windows RADIUS](#)

- Saída de depuração do VPN 3000 Concentrator

```
6 12/06/2000 09:33:03.910 SEV=4 PPTP/47 RPT=21 10.44.17.179
Tunnel to peer 10.44.17.179 established
```

```
7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179
```

```
8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23
```

```
9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser
```

```
11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [ baduser ]
disconnected.. failed authentication ( MSCHAP-V1 )
```

```
12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
```

- saída de log do Cisco Secure ACS para Windows

```
03/18/2000,08:02:47,Authen failed, baduser,,,CS user
unknown,,,1155,10.2.2.1
```

- A mensagem que o usuário vê (do Windows 98)

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

"Criptografia MPPE necessária" está selecionada no concentrador, mas o servidor Cisco Secure ACS for Windows não está configurado para MS-CHAP-MPPE-Keys e MS-CHAP-MPPE-Types

- Saída de depuração do VPN 3000 ConcentratorSe AUTHDECODE (1-13 Gravidade) e depuração PPTP (1-9 Gravidade) estiverem ativados, o registro mostra que o servidor Cisco Secure ACS para Windows não está enviando o atributo 26 específico do fornecedor (0x1A) no access-accept do servidor (registro parcial).

```
2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE .N,..u.16Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF ..//.....
```

```
2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
```

- A saída do registro do Cisco Secure ACS para Windows não mostra falhas.

- A mensagem que o usuário vê

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

[Informações Relacionadas](#)

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de suporte ao cliente do Cisco VPN 3000 Series](#)
- [Página de suporte do IPSec](#)
- [Cisco Secure ACS para página de suporte do Windows](#)
- [Página de suporte RADIUS](#)

- [Página de suporte do PPTP](#)
- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)